

# ► KASPERSKY SYSTEMS MANAGEMENT

## Effacité informatique et sécurité renforcée

Les responsables informatiques doivent relever de nombreux défis pour sécuriser leurs données et apporter un support technique de qualité à leurs utilisateurs. Malheureusement, chaque tâche peut nécessiter d'utiliser des applications ou des outils distincts provenant d'éditeurs différents. Les professionnels de l'informatique nous expliquent justement que l'un de leurs principaux défis est d'utiliser des outils qui n'ont jamais été conçus pour fonctionner ensemble. Des outils informatiques hétérogènes sont en effet sources de complexité et, comme chacun le sait, la complexité est l'ennemi de la sécurité.

Voici une présentation de Kaspersky Systems Management. Cette solution propose un vaste éventail d'outils de productivité informatique très puissants pour les environnements Windows, tous développés à partir du même code source et gérés à partir d'une seule et même console. Vous bénéficiez ainsi d'une plate-forme offrant la simplicité et l'automatisation dont vous rêvez et la sécurité et le contrôle dont vous avez besoin.

- Déploiement des systèmes d'exploitation
- Installation, distribution logicielle et dépannage à distance
- Détection et hiérarchisation automatisées des vulnérabilités
- Gestion des correctifs et distribution des mises à jour automatisées
- Contrôle d'accès au réseau
- Inventaires matériels et logiciels
- Gestion à distance depuis une seule console – Kaspersky Security Center

### BÉNÉFICES

#### RENFORCER LA SÉCURITÉ

La détection et la hiérarchisation automatiques en temps voulu des vulnérabilités des systèmes d'exploitation et des logiciels associées à une distribution rapide et automatique des correctifs et des mises à jour vous permet de bénéficier d'une sécurité accrue tout en allégeant votre charge administrative.

#### TRAVAILLER EFFICACEMENT

Les administrateurs peuvent distribuer et installer à distance des mises à jour, des correctifs et des applications. Le dépannage à distance leur évite également de perdre du temps au téléphone ou d'avoir à se déplacer de poste en poste pour résoudre un problème. Le déploiement centralisé et automatisé des systèmes d'exploitation permet en outre de réduire la charge de travail, les administrateurs n'ayant plus à reproduire les mêmes tâches pour configurer chaque poste utilisateur.

#### CONTRÔLE AVEC VISIBILITÉ TOTALE

Grâce à une visibilité complète du réseau depuis une console unique, les administrateurs peuvent surveiller chaque application et appareil, y compris les appareils des visiteurs entrant sur le réseau. Cette visibilité permet un contrôle centralisé de l'accès aux données et aux applications logicielles de l'entreprise par utilisateur ou appareil, conformément aux politiques informatiques.

#### ADMINISTRER DE MANIÈRE CENTRALISÉE

Ces fonctionnalités et bien d'autres encore font partie de Kaspersky Systems Management et sont toutes accessibles depuis la console d'administration Kaspersky Security Center. Une console centralisée permet de bénéficier de commandes homogènes et intuitives ne nécessitant pas de formation complémentaire.

## FONCTIONNALITÉS

### DÉPLOIEMENT D'APPLICATIONS ET DE SYSTÈMES D'EXPLOITATION

Simplicité de création, de stockage, de clonage et de déploiement des images système depuis un point unique. Permet de fournir aux utilisateurs des systèmes exempts de problèmes et bénéficiant de configurations de sécurité optimales, notamment le déploiement en dehors des heures de travail via Wake-On-LAN. Cet outil est parfaitement adapté à la migration des systèmes d'exploitation.

### DISTRIBUTION LOGICIELLE

Les logiciels peuvent être distribués et mis à jour à distance depuis une console unique. Plus de 100 applications parmi les plus utilisées, telles qu'identifiées avec Kaspersky Security Network, peuvent être installées et mises à jour automatiquement, en dehors des heures de travail le cas échéant, afin de simplifier davantage le processus de distribution. La solution prend intégralement en charge le dépannage à distance sur n'importe quel système client, depuis une console unique. La technologie multicast permet de désigner certains postes de travail de sites distants comme « agents centraux » pour la distribution locale des mises à jour, pour des déploiements logiciels plus rapides et moins gourmands en bande passante.

### INVENTAIRES MATÉRIELS ET LOGICIELS

Les PC, disques durs et même les appareils amovibles sont automatiquement identifiés et répertoriés. La connexion de tout nouvel appareil déclenche l'envoi d'une notification à l'administrateur, qui peut suivre le statut et l'utilisation du matériel sur le réseau. De la même façon, l'inventaire logiciel suit avec précision quels logiciels sont utilisés à tel ou tel moment, et peut être déployé conjointement avec les outils de contrôle des terminaux de Kaspersky Lab afin de bloquer ou de restreindre l'utilisation de certaines applications logicielles.

### DISTRIBUTION ET CONTRÔLE DES LICENCES

La visibilité du nombre d'utilisateurs d'une application à un moment donné permet d'identifier les utilisateurs en non-conformité et comment rationaliser les coûts liés aux licences.

### ÉVALUATION DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS

En un clic, les résultats de l'analyse des vulnérabilités matérielles et logicielles sont comparés avec différentes bases de données des vulnérabilités et automatiquement hiérarchisés afin de dégager les vulnérabilités prioritaires et celles qui peuvent attendre. Les correctifs et mises à jour peuvent ensuite être automatiquement déployés sur cette base, en mode à la demande ou en mode programmé.

### CONTRÔLE D'ACCÈS AU RÉSEAU

Le contrôle d'accès au réseau permet de contrôler l'accès des visiteurs de manière simple et directe. Les nouveaux appareils sur le réseau sont automatiquement identifiés et contrôlés sur la base de l'inventaire logiciel et des politiques de sécurité informatique. Les appareils présentant un risque se verront refuser l'accès au réseau, tandis que les appareils des visiteurs pourront être redirigés sur un portail captif et pourront accéder à Internet.

### ADMINISTRATION CENTRALISÉE

Les outils de Kaspersky Systems Management font partie d'une plate-forme de sécurité intégrée unique, offrant toutes les fonctions utiles de sécurité et d'administration informatiques à partir d'une même console de gestion baptisée Kaspersky Security Center. Kaspersky Security Center prend en charge l'administration de la sécurité des systèmes pour les ordinateurs de bureau, les terminaux mobiles et les terminaux virtuels présents sur le réseau de l'entreprise, et ce via une seule et même console, éliminant la complexité et renforçant la sécurité.

## Comment vous procurer ce produit ?

**Kaspersky Systems Management est un composant géré à partir de Kaspersky Security Center et est intégré aux versions suivantes :**

- Kaspersky Endpoint Security for Business — Advanced
- Kaspersky Total Security for Business

Vous pouvez également acheter Kaspersky Systems Management séparément en tant que solution ciblée. Contactez votre revendeur Kaspersky Lab pour en savoir plus sur ce produit et sa tarification.

**LES FONCTIONNALITÉS NE SONT PAS TOUTES DISPONIBLES SUR L'ENSEMBLE DES PLATES-FORMES.**  
Pour en savoir plus, rendez-vous sur [www.kaspersky.fr](http://www.kaspersky.fr)